Available online at www.sciencedirect.com
SciVerse ScienceDirect
Procedia Engineering 24 (2011) 128 – 132
Procedia Engineering
www.elsevier.com/locate/procedia

2011 International Conference on Advances in Engineering

Cryptanalysis of an efficient secret handshakes scheme with unlinkability

Eun-Jun Yoon*

School of Computer Engineering, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea

Abstract

In 2011, Gu-Xue proposed an improved secret handshakes scheme with unlinkability based on the Huang-Cao scheme that can achieve strong unlinkability against an outsider adversary. However, this paper points out that Gu-Xue scheme is insecure to key-compromise impersonation (K-CI) attack and cannot provide master key forward secrecy (MFS).

Keywords: Secret handshakes, unlinkability, key-compromise impersonation resilience, forward secrecy

1. Introduction

Unlinkable secret handshakes scheme provides unlinkability which means that an adversary cannot link any two different instances of same party ([1]). Therefore, unlinkability property has been recognized as a desirable security requirement in many applications such as group signatures, identity escrow, electronic-cash and unlinkable credentials. In 2007, Jarecki et al. ([2]) first proposed an unlinkable secret handshakes scheme. In 2009, Huang and Cao ([3]) proposed a novel and efficient unlinkable secret handshakes scheme that requires only constant exponentiations instead of the logarithm complexity. However, both Su ([4]) and Youn et al. ([5]) examined the security of the Huang-Cao scheme and then proved some security flaws of the scheme. Su ([4]) demonstrated that an adversary who did not register himself as a group user can successfully make a unlinkable secret handshaking with other registered users. Youn et al.

*Corresponding author. Tel.: +82-53-850-7291; Fax: +82-53-850-7609.
Email address: ejyoon@kiu.ac.kr (Eun-Jun Yoon)

1877-7058
doi:10.1016/j.proeng.2011.11.2614

([5]) showed that it fails to achieve two fundamental requirements such as the affiliation-hiding property and the authenticated key exchange (AKE) security.

In 2011, Gu-Xue ([6]) proposed an improved secret handshakes scheme with unlinkability based the on Huang-Cao scheme to overcome Youn et al.'s proposed attacks. Gu-Xue scheme is ID-based AKE scheme. Although, Gu-Xue scheme achieved strong unlinkability against an outsider adversary $\mathcal{A}$, the scheme cannot provide Key-compromise impersonation (K-CI) resilience and does not provide master key forward secrecy (MFS). K-CI resilience and MFS are important security requirements in ID-based two-party AKE scheme ([7, 8, 9, 10, 11]). They define as follows.

Definition 1. *Key-compromise impersonation (K-CI) resilience - Suppose legitimate entity U_A's private key is compromised. It is obvious that an adversary who knows this key to impersonate U_A to any other entity (e.g. U_B). However, compromising U_A's private key should not enable the adversary to impersonate any other entity (e.g. U_B) to U_A.*

Definition 2. *Forward secrecy (FS) - Long-term private keys's disclosure of one or more of the entities should not affect the secrecy of previous session keys established by honest entities. It can be considered as three cases from different levels of this property:*

1. *Partial forward secrecy: Compromising some but not all of the entities long-term keys can not disclose previously established session keys.*
2. *Perfect forward secrecy (PFS): Compromising all of the entities long-term keys can not disclose previously established session keys.*
3. *Master key forward secrecy (MFS): Compromising the master private key of the group administrator (GA) cannot affect the secrecy of previously established session keys. This is a particular property in the identity-based systems and it implies perfect forward secrecy.*

Therefore, this paper points out that Gu-Xue scheme is insecure to K-CI attack and cannot provide MFS based on the above definitions. Our cryptanalysis results are important for security engineers, who are responsible for the design and development of efficient and secure secret handshakes schemes with unlinkability.

2. Review of Gu-Xue scheme

This section briefly reviews the Gu-Xue scheme ([6]). The scheme is composed of three algorithms: CreateGroup, AdmitMember, and Handshakes. The following system parameters are used throughout this paper.

- k: Security parameter.
- G_1, G_2: Two cyclic groups of a large prime order q.
- $P, Q \in G_1$: Two generators of group G_1.
- $\hat{e} : G_1 \times G_1 \rightarrow G_2$: Bilinear pairing map if for any $a, b \in Z_q$, $P, Q \in G_1$, where $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- G_1^*: Non-identity elements set of G_1.
- $H_0 : \{0,1\}^* \rightarrow G_1^*$ and $H_1 : \{0,1\}^* \rightarrow \{0,1\}^k$: Two cryptographic hash functions.

The system $\texttt{params} = \{q, G_1, G_2, G_1^*, \hat{e}, k, P, Q, H_0, H_1\}$ are published.

2.1. CreateGroup

A group administrator GA creates a group $\mathcal{G}$ by selecting a random number $s \in \mathbb{Z}_q$ as the secret specific to $\mathcal{G}$. $\mathcal{G}$ is defined by the set of users belonging to $\mathcal{G}$.

2.2. AdmitMember

To admit user U_i into group $\mathcal{G}$, GA chooses a random string $id_i \leftarrow \{0,1\}^k$ and computes a long-term private key $S_i = sQ_i$ where $Q_i = H(id_i)$, and issues $cert_i = (id_i, S_i)$ to user U_i through anonymous and secure channel.

2.3. Handshakes

The interactions between two participants U_A, U_B who belong to two groups denoted by $\mathcal{G}_0$ and $\mathcal{G}_1$ respectively, are shown in Fig. 1. Each user's input is a couple $(cert, init/resp)$ where $cert$ is a certificate and $init/resp$ is the user's role in the scheme. Let $agree-on$ be a special symbol, different from $init$ and $resp$.

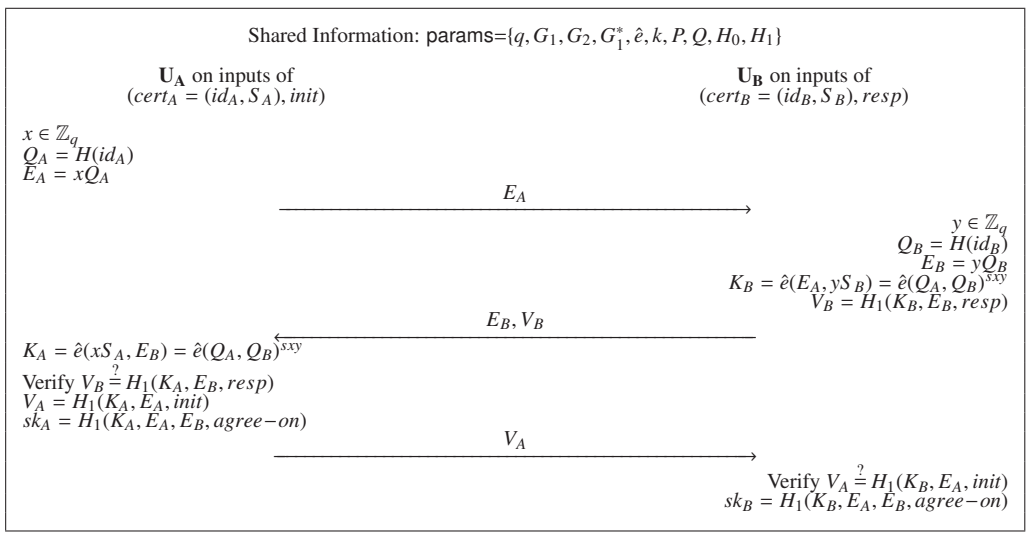

Figure 1: Gu-Xue's unlinkable secret handshakes scheme

3. Cryptanalysis of Gu-Xue's scheme

This section shows that Gu-Xue scheme is insecure to K-CI attack and does not provide MFS.

3.1. Key-Compromise Impersonation (K-CI) Attack

Gu-Xue scheme cannot withstand K-CI attack. Assume that the long-term private key $cert_A = (id_A, S_A)$ of U_A is disclosed to the adversary $\mathcal{A}$, which will then impersonate as U_B (it means any registered users of group $\mathcal{G}$) to U_A. In the proposed K-CI attack, $\mathcal{A}$ can compute valid E'_B and V'_B and then send them to U_A. Since the transmitted messages between the two participating parties contain the secret shared key $K_A = K'_B$; therefore, $\mathcal{A}$ can prepare a suitable message to impersonate the initiator party to any part of the network model as in the Gu-Xue's scheme:

1. U_A generates a random integer $x \in \mathbb{Z}_q$, computes $Q_A = H(id_A)$ and $E_A = xQ_A$, and then sends E_A to $\mathcal{A}$.
2. Upon receiving E_A from U_A, an adversary $\mathcal{A}$ computes Q_B, E'_B, K'_B and V'_B as follows:

$$Q_B = H(id_A) \tag{1}$$

$$E'_B = Q_A \tag{2}$$

$$K'_B = \hat{e}(S_A, E_A) = \hat{e}(Q_A, Q_A)^{sx} \tag{3}$$

$$V'_B = H_1(K'_B, E'_B, resp) \tag{4}$$

   Finally, $\mathcal{A}$ sends E'_B and V'_B to U_A.
3. Upon receiving E'_B and V'_B from $\mathcal{A}$, U_A will compute same secret shared key $K_A = \hat{e}(xS_A, E'_B) = \hat{e}(Q_A, Q_A)^{sx}$. U_A will verify whether $V'_B \stackrel{?}{=} H_1(K_A, E'_B, resp)$. Because they always hold, U_A will compute a message authentication value $V_A = H_1(K_A, E_A, init)$ and common session key $sk_A = H_1(K_A, E_A, E_B, agree-on)$. Finally, U_A will send V_A to $\mathcal{A}$.
4. Upon receiving V_A from U_A, $\mathcal{A}$ computes common session key sk'_B as follows:

$$sk'_B = H_1(K'_B, E_A, E'_B, agree-on) \tag{5}$$

   Because $\mathcal{A}$ is a dishonest party, it does not need to check the message authentication value V_A as the honest party; therefore, it accepts the computed value sk'_B as the session key.

Clearly, an adversary $\mathcal{A}$ can impersonate U_A to other parties in the group $\mathcal{G}$ using the long-term private key $cert_A = (id_A, S_A)$ of U_A; therefore, the Gu-Xue's scheme cannot withstand the K-CI attack as shown in Fig. 2.

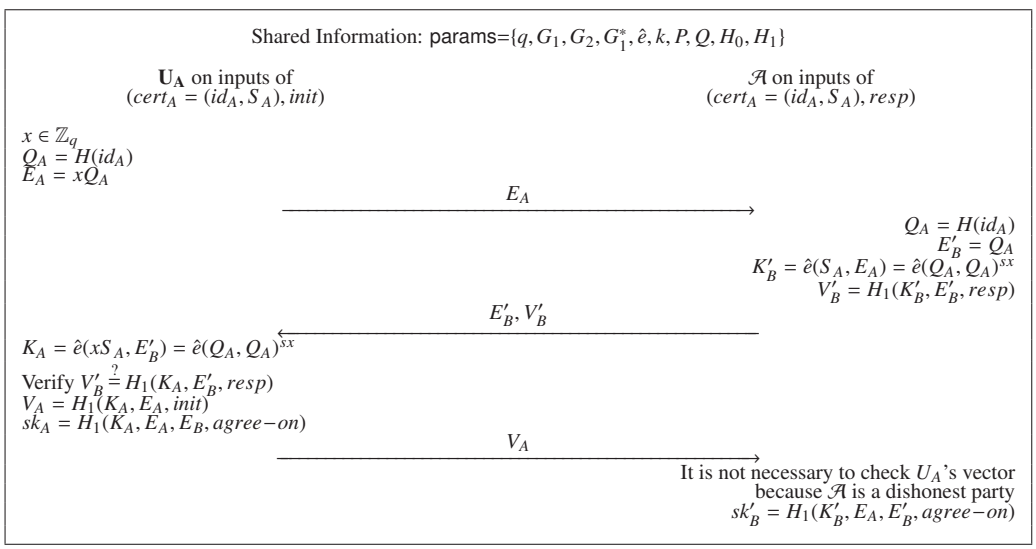

Figure 2: K-CI attack on Gu-Xue scheme.

3.2. Master Key Forward Secrecy (MFS) Problem

Gu-Xue scheme cannot provide MFS ([7, 8]). MFS is important security requirement in ID-based AKE scheme. That is, if the group administrator GA's secret key s is compromised, this should not compromise the previously established session keys sk. In the Gu-Xue scheme, if the long-term private keys S_A of U_A and S_B of U_B are compromised, the secrecy of previously established session keys $sk = H_1(K, E_A, E_B, agree–on)$ should not be affected without knowing x and y, where $K = K_A = K_B = \hat{e}(Q_A, Q_B)^{sxy}$. Therefore, Gu-Xue scheme provides perfect forward secrecy (PFS).

However, an adversary $\mathcal{A}$ which is not a registered group user can successfully make a unlinkable secret handshaking with other registered users. That is, $\mathcal{A}$ can simply compute the secret shared key K between U_A and U_B by using the group secret s of GA as follows:

$$K = \hat{e}(E_A, E_B)^s = \hat{e}(Q_A, Q_B)^{sxy} \tag{6}$$

where E_A and E_B are random numbers chosen by U_A and U_B, respectively. In addition, $\mathcal{A}$ can compute the common session key $sk = H_1(K, E_A, E_B, agree - on)$ by using the computed K and then freely impersonate U_A or U_B in the subsequent communications between U_A and U_B. Therefore, $\mathcal{A}$ can make a valid unlinkable secret handshaking with other registered user because of MFS problem in Gu-Xue scheme.

4. Conclusions

This paper pointed out that the Gu-Xue's efficient unlinkable secret handshakes scheme cannot withstand key-compromise impersonation (K-CI) attack and does not provide master key forward secrecy (MFS). For this reason, Gu-Xue scheme is insecure for practical application. It is important that security engineers should be made aware of this, if they are responsible for the design and development of secure unlinkable secret handshakes schemes.

References

[1] Balfanz D, Durfee G, Shankar N, Smetters D K, Staddon J, Wong H C, Secret handshakes from pairing-based key agreements. In Proc. IEEE Symposium on Security and Privacy, pp. 180-196, 2003.
[2] Jarecki S, Liu X, Unlinkable secret handshakes and key-privacy in group key management scheme, In Proc. ACNS'07, LNCS 4521, pp. 270-287, 2007.
[3] Huang H, Cao Z, A novel and efficient unlinkable secret handshakes scheme, IEEE Commun. Lett., Vol. 13, No.5, pp. 363-365, 2009.
[4] Su R, On the security of a novel and efficient unlinkable secret handshakes scheme, IEEE Commun. Lett., Vol. 13, No. 9, pp. 712-713, 2009.
[5] Youn T, Park Y, Security analysis of an unlinkable secret handshakes scheme, IEEE Commun. Lett., Vol. 14, No. 1, pp. 4-5, 2010.
[6] Gu J, Xue Z, An improved efficient secret handshakes scheme with unlinkability, IEEE Commun. Lett., Vol. 15, No. 2, pp. 259-261, 2011.
[7] Chen L, Kudla C, Identity based authenticated key agreement protocols from pairings, Cryptology ePrint Archive, Report 2002/184, Available at http://eprint.iacr.org/2002/184/.
[8] Choie Y, Jeong E, Lee E, Efficient identity-based authenticated key agreement protocol from pairings, Applied Mathematics and Computation, Vol. 162, No. 1, pp. 179-188, 2005.
[9] Al-Riyami S, Paterson K, Certificateless public key cryptography, In Proc. Asiacrypt'03, LNCS 2894, pp. 452-473, 2003.
[10] Mandt T, Tan C, Certificateless authenticated two-party key agreement protocols, In Proc. Asian'06, LNCS 4435, pp. 37-44, 2008.
[11] Zhang L, Zhang F, Wu Q, Domingo-Ferrer J, Simulatable certificateless two-party authenticated key agreement protocol, Information Sciences, Vol. 180, No. 6, pp. 1020-1030, 2010.